Stephen R. Cochell (SBN 145225)
srcochell@gmail.com
COCHELL LAW FIRM, P.C.
5850 San Felipe, Suite 500
Houston, Texas 77057
Admitted Pro Hac Vice

Allan Grant (SBN#213658)
Grant's Law Firm
17351 Greentree Drive
Riverside, California 92503-6762
Telephone (888)937-7555
Facsimile (866)858-6637

Attorneys for Defendant
JASON EDWARD THOMAS CARDIFF

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA, Plaintiff, vs. JASON EDWARD THOMAS CARDIFF, Defendant.	Case No. 5:23-CR-00021-JGB [*Filed concurrently with Declaration of Stephen R. Cochell, Jason Cardiff and [Proposed] Order*] Courtroom: 1 Hearing Date: October 21, 2024 Time: 2:00 PM

DEFENDANT JASON CARDIFF'S NOTICE OF MOTION AND MOTION TO DISMISS COUNT TWO OF THE INDICTMENT

NOTICE

TO ALL PARTIES AND ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on October 21, 2024, at 2 p.m. in the courtroom of the Honorable Jesus G. Bernal, United States District Judge, Defendant Jason Cardiff, by and through his attorneys of record, Stephen R. Cochell, hereby moves this Honorable Court for an order dismissing Count Two of the Indictment, which charges Aggravated Identity Theft, a violation of 18 U.S.C. § 1028A(a)(1).

This Motion is based upon the attached Memorandum of Points and Authorities, the Declaration of Stephen R. Cochell, the Declaration of Jason Cardiff, and all files and records in this case, and any further evidence as may be adduced at the hearing on this Motion.

This motion is made following the conference of counsel pursuant to L.R. 7-3, which took place on September 6, 2024.

Dated: September 9, 2024

By: /s/ Stephen R. Cochel
Stephen R. Cochell

Attorneys for Defendant
JASON EDWARD THOMAS CARDIFF

TABLE OF CONTENTS

INDEX OF AUTHORITIES

Case Law

Rules

Statutes

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

The Indictment charges Mr. Cardiff with, among other things, Aggravated Identity Theft, a violation of 18 U.S.C. § 1028A(a)(1). After the Indictment was filed, the Supreme Court decided *Dubin v. United States*, 599 U.S. 110 (2023), which significantly narrowed the reach of the Aggravated Identity Theft statute. Applying *Dubin*, Mr. Cardiff's prosecution for Aggravated Identity Theft cannot proceed, as his alleged conduct was the type of "garden variety" overbilling that the Supreme Court held was not penalized by the statute

A key component of aggravated identity theft, as clarified in *Dubin*, is the requirement of deception concerning "who" is involved in the transaction. The Supreme Court emphasized that identity theft occurs when a defendant uses another person's identification to deceive about the identity of the parties involved in the transaction. This means that the fraudulent use of identification must go to the heart of the deception, altering the perception of the identities of those involved. The crux of the healthcare fraud in *Dubin* was a misrepresentation about the qualifications of Dubin's employees. The *Dubin* court found that Dubin misrepresented how and when services were provided to a patient but he did not misrepresent *who* received the services. Thus, his use of a patient's identifying information did not fall within the meaning of § 1028A(a)(1). *Id.* at 132.

As in *Dubin*, there is no indication that Mr. Cardiff or Redwood Scientific Technologies used the customers' identities to deceive anyone about "who" was received the services. The identity of the customer as the purchaser and Redwood as the merchant remained clear and unaltered throughout the transactions. The alleged misconduct in this case pertains to "how" the transactions were processed, not to any misrepresentation of "who" was involved.

In addition to the fact that there was no misrepresentation as to the "who" in

the transactions in the instant case, the Government's § 1028A(a)(1) fails because neither Redwood nor Cardiff used credit card or debit card account numbers in the transactions. In *Dubin*, the Court rejected the Government's claim that Dubin's overbilling was facilitated by use of a Medicaid reimbursement number and therefore automatically fell within the definition of § 1028A(a)(1). *Id.* at 128. In this case, the credit card account numbers provided by Redwood customers were encrypted by a third party Customer Relationship Management ("CRM"). The account numbers were not accessible by Cardiff or Redwood staff. Unlike Mr. Dubin, who used Medicaid reimbursement numbers as an identifier, Redwood lacked access to customer credit card and debit card account numbers during January through April 2018.

The facts in this case fall squarely within the *Dubin* Court's analysis, holding that use of a means of identity (in that case Medicaid numbers) were simply a means to execute billing, but were not a tool for deception about the identity of the parties.

Accordingly, the Court should dismiss Count Two, which charges Mr. Cardiff with Aggravated Identity Theft.

II. STATEMENT OF FACTS

A. The Indictment

Mr. Cardiff is charged with three crimes: access device fraud under 18 U.S.C. § 1029(a)(5), aggravated identity theft under 18 U.S.C. § 1028A(a)(1), and witness tampering under 18 U.S.C. § 1512(b)(2)(B). (Indictment, Dkt. No. 1.) Only the first two offenses, contained in the first two counts, are relevant to this motion.

Count One, the access device fraud count, alleges that between January 22, 2018 and May 2018, Mr. Cardiff effected transactions with debit and credit card account numbers and expiration dates belonging to Redwood customers, and in doing so, obtained at least $1,000 during a one-year period.

Count Two, the aggravated identity theft count, alleges that between January 22, 2018 and May 2018, Mr. Cardiff transferred, possessed, and used names, credit card account numbers, and debit card account numbers during and in relation to the

access device fraud count.

B. The FTC Action

As the Court knows, the government began its investigation of Mr. Cardiff's company Redwood Scientific Technologies, Inc. ("Redwood") through a civil investigative demand issued by the Federal Trade Commission ("FTC"). (*See* Order Denying Defendant's Motion to Dismiss the Indictment, Dkt. No. 79 at 2-9.) The FTC thereafter filed a civil action against various defendants, including Mr. Cardiff, his wife, and Redwood. *See FTC v. Cardiff, et al.*, Case No. 5:18-CV-02104-DMG-PLA (C.D. Cal. 2018) (hereafter cited as "*FTC v. Cardiff"* and referred to as "FTC Action"). The FTC eventually moved for summary judgment, and in doing so, submitted a "Statement of Uncontroverted Facts and Conclusions of Law" ("SUF").[1] *FTC v. Cardiff*, Dkt. No. 423-3 (Aug. 6, 2020). The FTC's SUF was cited extensively in the order granting in part the FTC's motion for summary judgment. *FTC v. Cardiff*, Dkt. No. 511 (Oct. 9, 2020).

C. The FTC's Statement of Uncontroverted Facts Relevant to Count One and Two of the Indictment

The SUF has a section titled "Jason Cardiff's 'Straight Sales-to-Continuity' Initiative." That section has factual allegations the FTC submitted to the court in the *FTC v. Cardiff* action ("FTC Facts"). Those same assertions constitute the conduct alleged in Counts One and Two of the Indictment.[2] The pertinent FTC Facts are as alleged as follows:

In January 2018, Mr. Cardiff purportedly directed that brand new continuity

[1] Because the SUF is 308 pages, Defendant has provided an extract of the relevant portions. Counsel is prepared to file the entire document if needed.

[2] The FTC Facts contained in the FTC's Statement of Uncontroverted Facts are accepted as true solely for the purpose of adjudication of the instant motion under Federal Rule of Criminal Procedure 12(b). Mr. Cardiff otherwise reserves the right to contest the FTC Facts at all stages of these proceedings and, indeed, does contest such alleged facts.

orders should be created for customers who had previously made one-time "straight sale" purchases so that their debit and credit cards could be charged again and going forward on a recurring basis. **Exhibit A**, Declaration of Stephen Cochell (hereafter "Cochell Dec.") Ex. 1, SUF at ⁋ 839. Redwood allegedly did not contact these consumers or get their approval for additional charges. **Exhibit A**, Ex. 1, SUF at ⁋ 840. Redwood staff allegedly processed hundreds of these unauthorized transactions each day and reported their success and failure rates to Mr. Cardiff. **Exhibit A**, Ex. 1, SUF at ⁋ 841.

The Government also alleges, in some cases, customers' credit and debit cards had expired since their original orders had been placed. **Exhibit A,** Ex. 1, SUF ⁋ 842. Mr. Cardiff allegedly directed his employees to try changing the cards' expiration dates to see if that would allow the new charges to be processed. **Exhibit A**, Ex. 1, SUF ⁋ 843.

The FTC further alleged that Redwood staff continued converting straight-sale customers to continuity plans and charging them without authorization until April 2018. **Exhibit A,** Ex. 1, SUF ⁋ 845. Redwood allegedly processed unauthorized charges for more than 1,500 consumers through Jason Cardiff's straight-to-continuity initiative. **Exhibit A,** Ex. 1, SUF ⁋ 847.

D. PCI Compliance: Redwood Did Not Store or Have Access to Customer Credit Cards, Debit Cards or Other Identifiers.

Payment card industry (PCI) compliance is mandated by credit card companies to help ensure the security of credit card transactions in the payments industry.[3] PCI Investopedia. Payment card industry compliance refers to the technical and operational standards that businesses follow to secure and protect credit card data provided by cardholders and transmitted through card processing transactions. *Id.*

---

[3] Defendant requests the Court take judicial notice of https://www.investopedia.com/terms/p/pci-compliance.asp which provides an overview of PIC compliance and will be cited as "PCI Compliance-Investopedia."

Redwood customers engaged in transactions that were processed using a third-party Customer Relationship Management (CRM) system called Limelight, which was later known as "Sticky." **Exhibit B**, Declaration of Jason Cardiff ¶ 3_(hereafter "Cardiff Dec.") Limelight provided CRM services provided that the customer was PCI compliant. **Exhibit B**, Cardiff Dec. ¶ 4 . When a Redwood customer purchased a product, the transaction was primarily conducted online, with customers entering their payment information directly into the Redwood website. **Exhibit B**, Cardiff Dec. ¶5. The credit card information was then tokenized and securitized. *Id.* at ¶ 5. Once the credit card number is entered and submitted, the credit card information is tokenized and securitized and cannot be accessed by redwood personnel. *Id.* at ¶4. Purchases could also be made through the phone room. *Id.* at ¶ 6 The order would be entered into the Sticky system and then tokenized and securitized. *Id. at* ¶ 5.

The CRM acknowledged the order was successfully placed, exports the data to the shipping department with the product, amount of product and where to ship the product. *Id.* at ¶ 8. While reports may be generated for each customer, the credit card information is redacted. Id at ¶ 9.

During its investigation, the DOJ confirmed and amplified the above details. In an interview with the prosecutors and investigators in this case, Joanny Spina, Limelight's Office Operation Manager, stated that banks send information to processing banks to approve or deny a sale. Notably, the "Sticky" CRM system adhered to PCI compliance standards, ensuring that credit card details were securely tokenized and inaccessible to any individual within Redwood or its associated entities. **Exhibit A**, Cochell Dec., Spina MOI, Ex. 2 at 2-3, **Exhibit A**, Bogosian MOI, Exhibit 3 at 1 According Ms. Spina "Sticky".io, "the system works with company call centers, payment gateways, and fulfillment providers, such as Shipstation (which printed labels for shipping). **Exhibit A**, Ex. 1 at 2. Credit card numbers are protected by encrypting the middle numbers of the card. "Sticky" sees the card as encrypted when

extracting information" **Exhibit A**, Ex. 1 at 2.

The PCI compliance of the "Sticky" CRM system is akin to the secure transaction processing systems used by major online retailers such as Amazon. Once a customer's payment information is entered, it is immediately tokenized and securitized, rendering the actual credit card numbers inaccessible. This security measure ensures that even if overcharging occurred, it would not involve the unauthorized access or misuse of a customer's credit card details, as these details were never accessible to anyone within Redwood. This process was confirmed in the teleconference with "Sticky".io executives, where it was clarified that the system was structured to prevent access to sensitive customer information **Exhibit A**, Bagosian MOA, Ex. 3 at 1. Furthermore, Redwood also accepted payments through its phone room operations, where orders were similarly processed directly into the "Sticky" CRM system by phone representatives.

III. ARGUMENT

A. Legal Standard

"Rule 12(b) of the Federal Rules of Criminal Procedure permits any defense "which is capable of determination without the trial of the general issue" to be raised by pretrial motion." *U.S. v. Shortt Accountancy Corp.*, 785 F.2d 1448, 1452 (9th Cir. 1986). "A pretrial motion is generally 'capable of determination' before trial if it involves questions of law rather than fact. *Id.* "However, 'a district court may make preliminary findings of fact necessary to decide the questions of law presented by pre-trial motions so long as the court's findings on the motion do not invade the province of the ultimate finder of fact.'" *Id.* (citing *U.S. v. Jones*, 542 F.2d 661, 664 (6th Cir. 1976)). As such, Rule 12(b) allows a defendant may move to dismiss the pleadings on the basis of a "defect in the indictment or information" and a "failure to state an offense." Fed. R. Crim. P. 12(b)(3)(B)(v).

When a motion to dismiss an indictment is based on uncontested facts, the Court is "faced with a pure issue of law, which it ha[s] to decide because no good

cause existed to defer its ruling until trial." *U.S. v. Phillips*, 367 F.3d 846, 855 (9th Cir. 2004); *see also Id.* at n. 25 ("Because neither party contested the facts, the district court neither 'invade[d] the province of the" jury nor determined an element of the offense.'"), cited with approval in *U.S. v. Rojas-Pedroza*, 716 F.3d 1253, 1261 (9th Cir. 2013); *see also U.S. v. Carter*, 2006 WL 997867, at *2 (E.D. Cal., Apr. 17, 2006) ("The existence of undisputed facts obviates the need for the district court to make factual determinations properly reserved for a jury.").

For purposes of this Motion, and for the sake of argument, Cardiff assumes, that the FTC Facts proffered by the FTC in the FTC Action are true. Although "every publication of every branch of government of the United States" cannot "be treated as a party admission by the United States under Fed. R. Evid 801(d)(2)(D)[,]" statements made by a "relevant and competent section of the government" are admissible against the Government as an opposing party admission. *See U.S. v. Van Griffin*, 874 F.2d 634, 638 (9th Cir. 1989). In *Van Griffin*, the Ninth Circuit held that a pamphlet on sobriety testing created by the Department of Transportation ("DOT") was admissible against the Government as a party admission. *Id.* Recently, the Ninth Circuit affirmed and clarified its holding in *Van Griffen*, explaining that the DOT's statements were admissible against the Government because the prosecution involved a crime related to highway safety, which fell under the purview of the DOT. *See United States v. Mirabal*, 98 F.4th 981, 986 (9th Cir. 2024); *see also U.S. v. Western Titanium, Inc.*, 2010 WL 3988291, at *8 (S.D. Cal., Oct. 12, 2010) (finding that Defense Contract Management Agency ("DCMA")'s report may be admissible "as a party admission because the DCMA appears to be the relevant and competent government agency charged with the development of rules for defense suppliers to ensure that… supplies and services meet all performance requirements.").

Just as the DOT was the "relevant and competent" agency of the Government related to crimes involving highway safety in *Van Griffen*, here the FTC is the "relevant and competent" agency of the government related to crimes related to

consumer protection. As such, the FTC Facts can be imputed to the government and because Cardiff does not dispute the FTC Facts for purposes of this Motion, the Court can consider whether the FTC Facts fail to state an offense as a matter of law.

Similarly, witness interviews conducted by the government are admissible if proffered by the defendant to support his defense. Rule 803(8), Federal Rules of Evidence allows for admission of factual findings from a legally authorized investigation when used against the government in a criminal case, and neither the source of information nor other circumstances indicate a lack of trustworthiness. In the instant case, the DOJ investigators and lawyers conducted an interview of Joanny Spina, an Operations Manager for LimeLight/Sticky, as part of their investigation of Defendant in this case.

B. Count Two Must Be Dismissed Under the Supreme Court's Recent Decision in *Dubin*[4]

The aggravated identity theft statute provides that "[w]hoever, during and in

[4] Moreover, the Aggravated Identity Theft statute is unconstitutionally vague. As Justice Gorsuch's concurrence in *Dubin* explains, Section 1028A(a)(1) fails to provide even rudimentary notice of what it does and does not criminalize. *Id.* at 133. Because the terms "use" and "in relation to" can have numerous meanings and are not defined by the statute, individuals are left to guess about what "use" entails and what the necessary (or a fair) amount of relation to the enumerated offense is required. Such unconstitutional lack of clarity remains uncured by the majority opinion in *Dubin*. As Justice Gorsuch explains:

> When, exactly, is a "means of identification" "at the crux," "a key mover," or a "central role" player in an offense? No doubt, the answer "turns on causation, or at least causation often helps to answer the question." The Court agrees but stresses that "a causal relationship" of any kind will not suffice. At the same time, however, it studiously avoids indicating whether the appropriate standard is proximate cause or something else entirely novel. All of which gives rise to further questions. In virtually every fraud, a "means of identification" plays some critical role in the fraud's success—good luck committing a mail or wire fraud, for instance, without relying heavily on the name of the victim and likely the names of other third parties. Just how much "causation" must a prosecutor establish to sustain a § 1028A(a)(1) conviction? For that matter, how does one even determine the extent to which a "means

relation to" certain enumerated felonies, "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person, shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years." 18 U.S.C. § 1028A(a)(1). As relevant here, a means of identification includes names, credit cards, and debit cards.

The predicate felony charged in this case is access device fraud. That statute prohibits knowingly and with the intent to defraud, effecting transactions, with one or more access devices issued to another person or persons, to receive payment or any other thing of value during any one-year period the aggregate value of which is equal to or greater than $1,000. 18 U.S.C. § 1029(a)(5)

The access devices used to effect the transactions alleged in Count One (access device fraud) are the credit and debit card numbers charged in Count Two (aggravated identity theft).

After the Indictment was returned, the Supreme Court reined in the government's sweeping interpretation and use of the aggravated identity theft statute in *Dubin*. The Court narrowly interpreted the statute as reaching more limited conduct than had previously resulted in convictions for aggravated identity theft, including convictions previously upheld in this circuit.

In *Dubin*, the petitioner overbilled Medicaid by inflating the qualifications of an employee who performed a test and claiming a higher reimbursement based on those qualifications. *Dubin*, 599 U.S. at 114. While the test had been done by a junior "psychological associate, the petitioner billed Medicaid as if the test had been done by a licensed psychologist. *Dubin*, 599 U.S. at 114. In the bill he submitted to

---

> of identification" "caused" an offense, as compared to the many other necessary inputs?

Id. at 135 (citations omitted).

Medicaid, the petitioner included a patient's name and Medicaid reimbursement number. *Dubin*, 599 U.S. at 115. Because he misrepresented the employee's qualifications and overbilled Medicaid, the petitioner was convicted of the predicate offense of healthcare fraud. And because in the process of submitting the fraudulent bill, he used a "means of identification"—the patient's name—he was also convicted of aggravated identity theft under § 1028A. *Dubin*, 599 U.S. at 114-15.

The Supreme Court reversed the petitioner's conviction for Aggravated Identity Theft. In reaching its decision, the Supreme Court interpreted two provisions of the statute, "use" of another's means of identification, and "during and in relation to" a predicate crime.

As to "use," the Court reasoned that for someone to "knowingly … use[ ], without lawful authority, a means of identification of another person[,]" there must be deception going to "*who*" is involved in the transaction rather than just "*how*" or "*when*" services were provided. *Dubin*, 599 U.S. at 123. The Court explained that this is required because "identity theft is committed when a defendant uses the means of identification itself to defraud or deceive." *Id.* In other words, when a means of identification is used deceptively, this deception goes to "*who*" is involved in the transaction, rather than just "*how*" or "*when*" services were provided. Use of the means of identification must be at "the locus of [the criminal] undertaking," rather than merely ancillary to a crime. *Id.* at 123.

As for "in relation to," the Court explained that the means of identification must play a "central role" or be a "key mover" in the predicate offense. "This central role played by the means of identification, which serves to designate a specific person's identity, explains why we say that the 'identity' itself has been stolen." *Id.* at 123 (citing *United States v. Spears*, 729 F.3d 753, 756 (7th Cir. 2013) ("'identity theft' occurs when someone's 'identity has been stolen or misappropriated'). Based on this reasoning, the Court explained why the below specific examples resulting from the Government's interpretation of the statute did not sound like—and did not qualify

as—identity theft.

> If a lawyer rounds up her hours from 2.9 to 3 and bills her client using his name, the name itself is not specifically a source of fraud; it only plays an ancillary role in the billing process. The same is true for the waiter who substitutes one cut of meat for another; we might say the filet mignon's identity was stolen, perhaps, but not the diner's.

Id. at 122–23 (emphasis added).

Therefore, the Court concluded, "a defendant 'uses' another person's means of identification 'in relation to' a predicate offense when this use is at the crux of what makes the conduct criminal." The Court clarified that this requires more than a "causal relationship," such as facilitating the offense or being a but-for cause of its success. *Id.* at 131 (citing *Id.* at 135 (GORSUCH, J., concurring in judgment)). Instead, the means of identification must be used in a manner that is in and of itself fraudulent or deceptive, going to "*who*" is involved in the transaction. *Id.* at 131-32.[5]

Turning to the FTC Facts, Mr. Cardiff's misrepresentations went not to "*who*" he or Redwood was or *"who"* their customers were, but to the "*what*" and the "*when*"—i.e., whether the customer signed up for a one-time or monthly subscription for products sold by Redwood. In effectuating the alleged predicate crime of using the customers' access devices to charge for monthly subscriptions when they had placed a one-time order, Mr. Cardiff did not misrepresent his or Redwood's identity or use a customer's means of identification that fraudulently or deceptively went to "*who*" was involved in the transaction. While using those customers' names and credit

[5] In *United States v. Hong*, 938 F.3d 1040,1050-1051 (9th Cir. 2019), the Ninth Circuit reversed a conviction for aggravated identity theft applying the circuit's well-established rule interpreting the term "use" in limited context-specific ways. "To interpret 'use' broadly "could encompass every instance of specified criminal misconduct in which the defendant speaks or writes a third party's name." *Hong* at 1051 *citing United States v. Spears*, 729 F.3d 753, 756 (7th Cir. 2013).

and debit card numbers was necessary to charge them for the subscriptions, that causal relationship is not sufficient under *Dubin*. If it were, there would be "an automatic 2-year sentence for generic overbilling that happens to use ubiquitous payment methods." *Id.* at 129. *see also Id.* at 124 (decrying the government's broad reading of the statute as applying an "aggravated" label "to all manner of everyday overbilling offenses" that would make "everyday overbilling" "the most common trigger for § 1028A(a)(1)'s severe penalty"). Every offense of access device fraud, which necessarily requires the use of a person's account numbers like credit cards and debit cards, could also be prosecuted as Aggravated Identity Theft. That would run afoul of the Supreme Court's clear directive in *Dubin* to read the statute more narrowly than encompassing all ancillary features of billing using ubiquitous payment methods.

It would also make the "aggravated" part of the statute's title irrelevant. In *Dubin*, the Court looked to the title of the statute as providing important context and color to the terms "uses" and "in relation to." While the Court was careful to limit both the role that a title plays in statutory interpretation and the scenarios where a title may be relevant, it made clear that the Aggravated Identity Theft statute was one of those instances where its title provides meaningful—and determinative—context. *Id.* at 121-22. Significantly, the Court highlighted that Congress titled the criminal statute "Aggravated Identity Theft," which it observed typically applies when an offense "is made worse or more serious by circumstances such as violence, the presence of a deadly weapon, or the intent to commit another crime." *Id.* at 123. This suggests, the Court reasoned, that Congress had in mind "a particularly serious form of identity theft." Permitting the government to tack on the 2-year mandatory minimum sentencing enhancement to what is a garden variety overbilling case would read "aggravated" out of the statute.

On September 3, 2024, the Ninth Circuit handed down its decision in *United States v. Ovsepian*, No. 21-55515. *Ovsepian* was a case where defendant allegedly "possessed" one patient file as part of an alleged conspiracy to commit health care

using Medicare and Medi-Cal identifying information. The Ninth Circuit reversed Ovsepian's 1028A conviction based on *Dubin*. In pertinent part, the Court reiterated that criminal liability under 18 U.S.C. § 1028A did not apply unless the use or possession of another's identifying information was at the "crux" of the fraudulent conduct, rather than an ancillary feature. *Ovsepian* at 25. The Court held that retention of a patient file may have been helpful in the event of an audit, but it was merely an "ancillary" feature of the scheme that merely facilitated its commission. *Id.* at 26 citing Dubin at 132. In Mr. Cardiff's case, any use of customer credit card information was purely incidental to the alleged billing errors and did not constitute deception regarding "who" was involved in the transaction.

Multiple courts have resolved motions invoking *Dubin* to challenge aggravated identity theft prosecutions or convictions. The courts that have affirmed Aggravated Identity Theft convictions have typically involved cases where the defendants passed themselves off as another person—for example, by forging the signature of another person or applying for identity documents using someone else's identity—to defraud a third party like a bank or government office. *See, e.g.*, *United States v. Felch*, No. 21-CR-0570, 2024 WL 406554, at *1–5 (D.N.M. Jan. 22, 2024) (upholding defendant's conviction for aggravated identify theft with a predicate offense of bank fraud where the defendant forged her employer's signature on a company check made payable to the defendant's credit card company). *Cf. United States v. Noble*, No. 1:23-CR-00165-SDG, 2024 WL 253623, at *4–5 (N.D. Ga. Jan. 23, 2024) (holding that Section 1028A requires an identity to have been "stolen or misappropriated").

In contrast, here, the FTC Facts reflect that Mr. Cardiff did not pass himself off as another person. He did not misrepresent his identity. He did not hold himself out as a customer or anyone else using a customer's means of identification. He did not use the customers' means of identification to defraud or deceive third parties. He held himself out as a merchant of the goods that had, in fact, been purchased by the customers. He was himself, his customers were his customers; at most this was a

garden variety case of overbilling or overprocessing the credit and debit cards in question. Moreover, Mr. Cardiff did not possess any of the credit card or debit card information.

Mr. Cardiff's conduct cannot be meaningfully distinguished from the fact scenarios used by the Dubin court ruling out aggravated identity theft under the statute. For example, the lawyer who bills her client electronically for three hours when she only worked 2.9 hours. The lawyer charged her client's account, with the client's name and account number, to effectuate the fraud. And by doing so, the lawyer implicitly represented to the client that she had done three hours of work and represented to the bank that the client had authorized the transaction representing three hours of billable time. If, as the Supreme Court indicated, the lawyer did not commit aggravated identity theft, then Mr. Cardiff did not either. Mr. Cardiff used encrypted data provided by customers to the CRM which billed customers for monthly subscriptions even if some of the customers originally placed one-time orders. The encrypted data was necessary to effectuate the charges but use of the data was ancillary to the crux of any fraud.

As with the examples provided by the Supreme Court, Redwood's customers' names and the encrypted credit and debit numbers were ancillary features of billing. Those encrypted account numbers were certainly necessary to effectuate the transactions, as charged in Count One, but there was no act of deceit going to "*who*" was involved in the transaction. Reading *Dubin* to permit the government to proceed with an aggravated identity theft prosecution under these facts would be contrary to *Dubin*'s clear rejection of an overbroad reading of the statute. *See Id.* at 129 ("So long as the criteria for the broad predicate offenses are met, the Government's reading creates an automatic 2-year sentence for generic overbilling that happens to use ubiquitous payment methods.").

IV. CONCLUSION

In light of the Supreme Court's decision in *Dubin v. United States*, which

narrowed the interpretation of aggravated identity theft under 18 U.S.C. § 1028A, it is clear that Mr. Cardiff's alleged conduct does not meet the statutory requirements for aggravated identity theft. The *Dubin* Court held that, for a defendant to be convicted of aggravated identity theft, the misuse of a person's means of identification must be central to the fraudulent conduct.

In Redwood's case, the use of credit card numbers was not central to the alleged fraud. The *Dubin* decision made clear that for identity theft to occur, the misuse of identifying information must directly relate to the deception about "who" is involved in the transaction, not merely "how" the transaction is processed. In Redwood's case, the overcharging—if it occurred—did not involve the deceptive use of credit card numbers to misrepresent the identity of the parties involved. Instead, these credit card numbers were securely stored and never accessed, and the transactions in question were processed within the confines of a system designed to prevent unauthorized access to such sensitive information. This is further evidenced by the "Sticky".io system's design, which explicitly prevented access to the underlying credit card information, as noted in the government's memorandum of activity**.**

The role of the credit card numbers in this situation were purely ancillary; they were necessary for processing payments, but they did not play a central, deceitful role in any alleged fraud. Any billing discrepancies that arose were related to the management of transactions, such as mistakenly placing customers on a recurring billing cycle, rather than to the misuse of a customer's identity.

This distinction is critical. Transactional errors, such as overbilling, are not equivalent to identity theft. Under *Dubin*, identity theft requires the misuse of a means of identification in a way that is fundamental to the fraud—something that did not occur in the operations at Redwood. Therefore, the conduct alleged in this case, even if proven, would not constitute aggravated identity theft, as the credit card numbers were not used in a manner that was central to any deceptive or fraudulent activity.

WHEREFORE, based on the foregoing, Mr. Cardiff respectfully requests that the Court dismiss Count Two of the Indictment with prejudice.

Respectfully submitted,

/s/ Stephen R. Cochell
Stephen R. Cochell
SBN: 24044255
The Cochell Law Firm, P.C.
5850 San Felipe, Ste 500
Houston, Texas 77057
(346) 800-3500 – Telephone
srcochell@gmail.com

SERVICE LIST

I HEREBY DECLARE THAT THE FOLLOWING COUNSEL HAVE BEEN SERVED WITH THIS DEFENDANT JASON CARDIFF'S NOTICE OF MOTION AND MOTION TO DISMISS COUNT TWO OF THE INDICTMENT THROUGH THE COURT'S ECF OR NEXT GEN ELECTRONIC FILING SYSTEM:

E. Martin Estrada
United States Attorney
Mack E. Jenkins
Assistant United States Attorney Chief, Criminal Division
Ranee A. Katzenstein
Assistant United States Attorney Chief, Criminal Division
Valerie Makarewicz
Assistant United States Attorney Major Frauds Section
1100 United States Courthouse
312 North Spring Street
Los Angeles, CA 90012
Telephone: (213) 894-0756 Facsimile: (213) 894-6269
E-mail: Valerie.Makarewicz@usdoj.gov

Amanda Liskamm
Director, Consumer Protection Branch Manu J. Sebastian
Brianna M. Gardner
Trial Attorneys
Consumer Protection Branch
U.S. Department of Justice
450 Fifth Street NW, Suite 6400 Washington, DC 20001
Telephone: (202) 514-0515 Facsimile: (202) 514-8742
E-mail: Manu.J.Sebastian@usdoj.gov
Brianna.M.Gardner@usdoj.gov

/S/ Stephen R. Cochell
Stephen R. Cochell